

What is claimed is:

- 1        1.     A system for providing passive screening of transient messages in  
2 a distributed computing environment, comprising:
  - 3        a network interface passively monitoring a transient packet stream at a  
4 network boundary comprising receiving incoming datagrams structured in  
5 compliance with a network protocol layer;
  - 6        a packet receiver reassembling one or more of the incoming datagrams  
7 into a segment structured in compliance with a transport protocol layer; and
  - 8        an antivirus scanner scanning contents of the reassembled segment for a  
9 presence of at least one of a computer virus and malware to identify infected  
10 message contents.
- 1        2.     A system according to Claim 1, further comprising:
  - 2        an incoming queue staging each incoming datagram intermediate to  
3 reassembly.
- 1        3.     A system according to Claim 1, further comprising:
  - 2        a network protocol-specific decoder decoding the reassembled segment  
3 prior to scanning.
- 1        4.     A system according to Claim 1, wherein the antivirus scanner  
2 terminates the transient packet stream if the reassembled segment is not infected  
3 with at least one of a computer virus and malware.
- 1        5.     A system according to Claim 1, wherein the antivirus scanner takes  
2 an action if the reassembled segment is infected with at least one of a computer  
3 virus and malware.
- 1        6.     A system according to Claim 5, wherein the action comprises at  
2 least one of logging an infection; generating a warning; spoofing a valid datagram  
3 in place of the infected datagram; and acquiescing to the infection.
- 1        7.     A system according to Claim 1, further comprising:

2 a protocol-specific queue staging each reassembled segment with other  
3 reassembled segments sharing the same transport protocol layer.

1 8. A system according to Claim 7, further comprising:  
2 an information record storing information dependent on the same transport  
3 protocol layer with the staged reassembled segment.

1 9. A system according to Claim 8, further comprising:  
2 a contents record storing the contents with the staged reassembled  
3 segment.

1 10. A system according to Claim 8, wherein the information comprises  
2 at least one of a source address, source port number, destination address,  
3 destination port number, URL, file name, user name, sender identification,  
4 recipient identification, and subject.

1 11. A system according to Claim 1, further comprising:  
2 a protocol-specific module processing each reassembled datagram based  
3 on the transport layer protocol employed by the reassembled datagram.

1 12. A system according to Claim 11, wherein the transport layer  
2 protocol comprises at least one of HTTP, FTP, SMTP, POP3, NNTP, and  
3 Gnutella.

1 13. A system according to Claim 1, further comprising:  
2 an event correlator analyzing the transient packet stream for events  
3 indicative of a network service attack.

1 14. A system according to Claim 13, further comprising:  
2 a data repository maintaining each event.

1 15. A system according to Claim 1, wherein the distributed computing  
2 environment is TCP/IP-compliant and each incoming message is SMTP-  
3 compliant.

1        16. A method for providing passive screening of transient messages in  
2 a distributed computing environment, comprising:

3            passively monitoring a transient packet stream at a network boundary  
4 comprising receiving incoming datagrams structured in compliance with a  
5 network protocol layer;

6            reassembling one or more of the incoming datagrams into a segment  
7 structured in compliance with a transport protocol layer; and

8            scanning contents of the reassembled segment for a presence of at least  
9 one of a computer virus and malware to identify infected message contents.

1        17. A method according to Claim 16, further comprising:  
2            staging each incoming datagram intermediate to reassembly.

1        18. A method according to Claim 16, further comprising:  
2            decoding the reassembled segment prior to scanning.

1        19. A method according to Claim 16, further comprising:  
2            terminating the transient packet stream if the reassembled segment is not  
3 infected with at least one of a computer virus and malware.

1        20. A method according to Claim 16, further comprising:  
2            taking an action if the reassembled segment is infected with at least one of  
3 a computer virus and malware.

1        21. A method according to Claim 20, further comprising:  
2            executing the action, comprising at least one of:  
3            logging an infection;  
4            generating a warning;  
5            spoofing a valid datagram in place of the infected datagram; and  
6            acquiescing to the infection.

1        22. A method according to Claim 16, further comprising:

2           staging each reassembled segment with other reassembled segments  
3       sharing the same transport protocol layer.

1           23.    A method according to Claim 22, further comprising:  
2            storing information dependent on the same transport protocol layer with  
3       the staged reassembled segment.

1           24.    A method according to Claim 23, further comprising:  
2            storing the contents with the staged reassembled segment.

1           25.    A method according to Claim 23, wherein the information  
2       comprises at least one of a source address, source port number, destination  
3       address, destination port number, URL, file name, user name, sender  
4       identification, recipient identification, and subject.

1           26.    A method according to Claim 16, further comprising:  
2            processing each reassembled datagram based on the transport layer  
3       protocol employed by the reassembled datagram.

1           27.    A method according to Claim 26, wherein the transport layer  
2       protocol comprises at least one of HTTP, FTP, SMTP, POP3, NNTP, and  
3       Gnutella.

1           28.    A method according to Claim 16, further comprising:  
2            analyzing the transient packet stream for events indicative of a network  
3       service attack.

1           29.    A method according to Claim 28, further comprising:  
2            maintaining each event in a data repository.

1           30.    A method according to Claim 16, wherein the distributed  
2       computing environment is TCP/IP-compliant and each incoming message is  
3       SMTP-compliant.

1           31. A computer-readable storage medium holding code for performing  
2 the method according to Claims 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28,  
3 29, or 30.

1           32. A system for passively detecting computer viruses and malware  
2 and denial of service-type network attacks in a distributed computing  
3 environment, comprising:

4           a network interface receiving copies of datagrams transiting a boundary of  
5 a network domain into an incoming packet queue, each datagram being copied  
6 from a packet stream;

7           a packet receiver reassembling one or more such datagrams from the  
8 incoming packet queue into network protocol packets, each staged in a  
9 reassembled packet queue;

10           an antivirus scanner scanning each network protocol packet from the  
11 reassembled packet queue to ascertain an infection of at least one of a computer  
12 virus and malware; and

13           an event correlator evaluating events identified from the datagrams in the  
14 packet stream to detect a denial of service-type network attack on the network  
15 domain.

1           33. A system according to Claim 32, further comprising:

2           a parser parsing each reassembled datagram into network protocol-specific  
3 information and packet content.

1           34. A system according to Claim 33, wherein the network protocol-  
2 specific information comprises a source address, source port number, destination  
3 address, destination port number, and URL for HTTP; a file name and user name  
4 for FTP; and a sender identification, recipient identification, and subject for  
5 SMTP.

1           35. A system according to Claim 33, further comprising:

2           a decoder decoding the packet content prior to performing the operation of  
3   scanning.

1           36.    A system according to Claim 32, further comprising:  
2           a log logging an occurrence of at least one of the infection and the network  
3   attack.

1           37.    A system according to Claim 32, further comprising:  
2           a warning module generating a warning responsive to an occurrence of at  
3   least one of the infection and the network attack.

1           38.    A system according to Claim 32, further comprising:  
2           a spoof module sending a spoofed network protocol packet responsive to  
3   an occurrence of at least one of the infection and the network attack.

1           39.    A system according to Claim 32, further comprising:  
2           one or more protocol-specific modules implementing one of HTTP, FTP,  
3   SMTP, POP3, NNTP, and Gnutella network protocols.

1           40.    A system according to Claim 32, wherein the distributed  
2   computing environment is TCP/IP-compliant, each datagram is IP-compliant, and  
3   each network protocol packet is TCP-compliant.

1           41.    A method for passively detecting computer viruses and malware  
2   and denial of service-type network attacks in a distributed computing  
3   environment, comprising:

4           receiving copies of datagrams transiting a boundary of a network domain  
5   into an incoming packet queue, each datagram being copied from a packet stream;  
6           reassembling one or more such datagrams from the incoming packet queue  
7   into network protocol packets, each staged in a reassembled packet queue;  
8           scanning each network protocol packet from the reassembled packet queue  
9   to ascertain an infection of at least one of a computer virus and malware; and  
10          evaluating events identified from the datagrams in the packet stream to  
11   detect a denial of service-type network attack on the network domain.

1           42.    A method according to Claim 41, further comprising:  
2            parsing each reassembled datagram into network protocol-specific  
3            information and packet content.

1           43.    A method according to Claim 42, wherein the network protocol-  
2            specific information comprises a source address, source port number, destination  
3            address, destination port number, and URL for HTTP; a file name and user name  
4            for FTP; and a sender identification, recipient identification, and subject for  
5            SMTP.

1           44.    A method according to Claim 42, further comprising:  
2            decoding the packet content prior to performing the operation of scanning.

1           45.    A method according to Claim 41, further comprising:  
2            logging an occurrence of at least one of the infection and the network  
3            attack.

1           46.    A method according to Claim 41, further comprising:  
2            generating a warning responsive to an occurrence of at least one of the  
3            infection and the network attack.

1           47.    A method according to Claim 41, further comprising:  
2            sending a spoofed network protocol packet responsive to an occurrence of  
3            at least one of the infection and the network attack.

1           48.    A method according to Claim 41, further comprising:  
2            implementing at least one of HTTP, FTP, SMTP, POP3, NNTP, and  
3            Gnutella network protocols.

1           49.    A method according to Claim 41, wherein the distributed  
2            computing environment is TCP/IP-compliant, each datagram is IP-compliant, and  
3            each network protocol packet is TCP-compliant.

1           50. A computer-readable storage medium holding code for performing  
2 the method according to Claims 41, 42, 43, 44, 45, 46, 47, 48, or 49.